UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/800,983	03/15/2004	G. Glenn Henry	CNTR.2073	1410

23669 7590 03/16/2009
HUFFMAN LAW GROUP, P.C.
1900 MESA AVE.
COLORADO SPRINGS, CO 80906

EXAMINER	
TRAORE, FATOUMATA	
ART UNIT	PAPER NUMBER
2436	

NOTIFICATION DATE	DELIVERY MODE
03/16/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PTO@HUFFMANLAW.NET

Office Action Summary	Application No.	Applicant(s)	
	10/800,983	HENRY ET AL.	
	Examiner	Art Unit	
	FATOUMATA TRAORE	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 December 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6,22-25 and 8020* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6, 8-20, 22-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the amendment filed December 28, 2008. Claims 1, 8, 17 and 22 have been amended. Claims 7, 16, 21 and 26 have been cancelled. Claims 1-6, 8-15, 17-20 and 22-25 are pending and have been considered below.

Claim Objections

2. Claim1 is objected to because of the following informalities: claim 1 recites the limitation of "a x86-compatible microprocessor", which should read "an x86-compatible microprocessor". Appropriate correction is required.

Claim Rejections - 35 USC § 112

3. The rejection has been withdrawn in light of the argument.

Specification

4. The object has been withdrawn in light of the amendment to the disclosure.

Response to Arguments

5. Applicant argues, "Applicant submits that a single x86-formated cryptographic instruction as part of an application program which is executed by an x86-compatible microprocessor according to the present invention is not contemplated by either one of the cited references, alone or in combination. A specific disclosure of an x86-compatible microprocessor is provided in the instant specification in numerous paragraphs, with the

following example from paragraph [0044] provided below for ease of ..... is thus a feature of the present invention to allow for use of the cryptographic instruction at the application level (i.e., within an application program as opposed to an operating system call), thus overcoming the disadvantages of present day coprocessor implementations", the examiner has provide a new ground of rejection to address the amended claims language. Juffa (US 6,247,117) disclose a crypto processing system where the crypto processor performs execution of application programs using an x86 compatible microprocessor.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1-6, 8-15, 17-20, 22-25 rejected under 35 U.S.C. 103(a) as being unpatentable over Kessler et al (US 6,789,147) in view of Juffa (US 6,247,117).

Claims 1, 17 and 22: Kessler et al disclose an apparatus and a method for performing cryptographic operations, comprising:

X86-compatible microprocessor, comprising:

i. An instruction register within a x86-compatible microprocessor (*Fig. 1, item 10*) having a cryptographic instruction disposed therein, wherein said cryptographic instruction is arranged according to the instruction

format for execution on said x86- compatible microprocessor, (*column 3, lines 40-45*) and wherein said cryptographic instruction is part of an application program, and wherein said x86-compatible microprocessor executes said application program, and wherein said cryptographic instruction prescribes one of the cryptographic operations, and wherein said cryptographic instruction prescribes that a user-generated key schedule be employed for execution of said one of the cryptographic operations (*the execution units include a plurality of operation blocks that correspond to different cryptographic operations that are used depending upon the type of instruction received in the execution queue. The operation blocks correspond to cryptographic algorithms such as AES, 3DES, DES, and RC4) (column 9, lines 8-42; Fig. 8);*

ii. A keygen unit, operatively coupled to said instruction register, configured to direct said x86-compatible microprocessor to load said user-generated key schedule *(column 12, lines 7-40)*; and

iii. An execution unit, operatively coupled to said keygen unit, configured to employ said user-generated key schedule to execute said one of the cryptographic operations (*column 9, lines 7-43*), said execution unit comprising:

A cryptography unit, configured execute a plurality of cryptographic rounds on each of a plurality of input text blocks to generate a corresponding each of a plurality of output text blocks, wherein said

plurality of cryptographic rounds are prescribed by a control word that is provided to said *cryptography unit (The primitive security operation blocks include an Advanced Encryption Standard (AES) block 807, a Triple Data Encryption Standard (3DES) block 809, a modular exponentiation block 811, a hash block 813, a simple arithmetic and logic block 815, and an alleged RC4.RTM. block 819) (column 9, lines 8-22).*

Kessler el al do not explicitly specify wherein said cryptographic instruction is part of an application program, and wherein said x86-compatible microprocessor executes said application program. However Juffa disclose an apparatus and method, which further disclose wherein said cryptographic instruction is part of an application program, and wherein said x86-compatible microprocessor executes said application program(column 8, lines 1-5; *column 17, lines 30-45; column 23, lines 3-8; Fig. 11, items 10 and 404*). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Kessler et al such as to use the x86-compatible microprocessor to execute the actual application program. The motivation of doing so would have been in order to detect special and exceptional cases of defined data format in advantageous as taught by Juffa (column 2, lines 55-65).

Claim 2: Kessler et al and Juffa disclose an apparatus for performing cryptographic operation as in claim 1 above, and Kessler et al further disclose wherein said one of the cryptographic operations further comprises:

An encryption operation, said encryption operation comprising encryption of a plurality of plaintext blocks to generate a corresponding plurality of ciphertext blocks*(step of performing cryptographic operations such encrypt operation and the decrypt operation) (column 7, line 54 to column 8, line10; Fig. 5 and Fig. 8)*.

Claim 3: Kessler et al and Juffa disclose an apparatus for performing cryptographic operation as in claim 1 above, and further Kessler et al disclose wherein said one of the cryptographic operations further comprises:

A decryption operation, said decryption operation comprising decryption of a plurality of ciphertext blocks to generate a corresponding plurality of plaintext blocks *(step of performing cryptographic operations such encrypt operation and the decrypt operation) (column 7, line 54 to column 8, line10; Fig. 5 and Fig. 8)*.

Claims 4, 18 and 24: Kessler et al and Harrison et al disclose an apparatus and a method for performing cryptographic operation as in claims 1, 17 and 22 above, and Kessler et al further discloses , wherein said user-generated key schedule is stored in memory(*Fig. 2*).

Claims 5, 19 and 25: Kessler et al and Juffa disclose an apparatus and method for performing cryptographic operation as in claims 1, 17 and 22 above, and Kessler et al further disclose, wherein said user-generated key schedule comprises an expanded key schedule according to the Advanced Encryption

Standard (AES) algorithm (*the operation blocks correspond to cryptographic algorithms such as AES, 3DES, DES and RC4)(Fig. 8*).

Claims 6, 20 and 23*:* Kessler et al and Juffa disclose an apparatus and a method as in claims 1, 17 and 22 above, and Kessler et al further disclose that said keygen unit is configured to interpret a key generation field within a control word, which is referenced by said cryptographic instruction *(column 12, lines 7-33)*.

Claim 8*:* Kessler et al and Harrison et al disclose an apparatus as in claim 1 above and Kessler et al further disclose that said cryptographic instruction implicitly references a plurality of registers within said x86-compatiblemicroprocessor (*execution unit) (column 9, lines 18-40; Fig. 8*).

Claims 9-11*:* Kessler et al and Juffa disclose an apparatus as in claim 8 above, and Kessler et al further disclose that said cryptographic instruction implicitly references a plurality of registers, which include a first register, wherein contents of said first register comprise a first pointer to a first memory address, said first memory address specifying a first location in memory for access of a plurality of input text blocks upon which said one of the cryptographic operations is to be accomplished ; and a second register wherein contents of said second register comprise a second pointer to a second memory address, said second memory address specifying a second location in said memory for storage of a corresponding plurality of output text blocks, said corresponding plurality of output text blocks being generated as a result of accomplishing said one of the

cryptographic operations upon a plurality of input text blocks said third register indicate a number of text blocks within a plurality of input text blocks (*each execution unit includes a register file block that includes data to be operated on by the corresponding cryptographic algorithm) (column 9, lines 18-40; Fig. 8)*.

Claim 12*:* Kessler et al and Harrison et al disclose an apparatus as in claim 8 above, and further Kessler et al further disclose that said plurality of registers comprises a fourth register, wherein contents of said fourth register comprise a third pointer to a third memory address, said third memory address specifying a third location in memory for access of cryptographic key data for use in accomplishing said one of the cryptographic operations (*column 9, lines 18-40; Fig. 5 and Fig. 8)*.

Claim 13*:* Kessler et al and Juffa disclose an apparatus and a method as in claim 8 above, and Kessler et al further disclose that said user-generated cryptographic key schedule comprises said cryptographic key data *(column 12, lines 8-32*).

Claim 14: Kessler et al and Juffa disclose an apparatus as in claim 8 above, and Kessler et al further disclose that said plurality of registers comprises a fifth register, wherein contents of said fifth register comprise a fourth pointer to a fourth memory address, said fourth memory address specifying a fourth location in memory, said fourth location comprising said initialization vector location, contents of said initialization vector location comprising an initialization vector or initialization vector equivalent for use in accomplishing said one of the

cryptographic operations(*cryptographic operation such as RC4) (column 9, lines 18-40; Fig. 5 and Fig. 8)*.

Claim 15: Kessler et al and Juffa disclose an apparatus as in claim 8 above, and Kessler et al further disclose that said plurality of registers comprises a sixth register, wherein contents of said sixth register comprise a fifth pointer to a fifth memory address, said fifth memory address specifying a fifth location in memory for access of a control word for use in accomplishing said one of the cryptographic operations, wherein said control word prescribes cryptographic parameters for said one of the cryptographic operations, and wherein said control word comprises: a key size field *(nk = key size)*, configured to specify said one of a plurality of cryptographic key sizes to be employed during execution of said one of the cryptographic operations*((cryptographic operation such as RC4) (column 9, lines 18-40; Fig. 5 and Fig. 8)*. The examiner notes that it is inherent for the control word to be stored in memory because the key expansion block uses it for generating a round key.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571) 270-1685. The examiner can normally be reached Monday through Thursday from 7:00 a.m. to 4:00 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nassar G. Moazzami, can be reached on (571) 272 4195. The fax phone

number for Formal or Official faxes to Technology Center 2100 is (571) 273-8300. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (571) 270-2685.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

2. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Monday, March 9, 2009

/F. T./

Examiner, Art Unit 2436

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2436